CS4677 Computer Forensics

Chris Eagle

Fall '06

Who Am I

- Chris Eagle, x2378, S-530C
  cseagle@nps.edu
- CS Senior Lecturer
- Director, Computer Network Research Lab
- Interests
  - Computer Network Attack/Defense/Exploitation
  - Reverse Engineering

Course Description

CS4677 Computer Forensics (3-2). This course is intended to provide students with an understanding of the **fundamentals of computer forensics** as it might be used in the context of DoN/DoD information assurance and information operations activities. Students will examine how **information** is stored in computer systems and how it may be deliberately **hidden** and **subverted**. The course will establish a sound foundation based upon methods for **information extraction as used for evidential purposes**. It will cover **practical forensic examination and analysis**. The course will also examine techniques of computer **evidence recovery** and the successful presentation of such evidence within legal contexts. Laboratory activities will introduce students to the use of common forensic tools, the principle of original integrity, disk examination, logging and preparation of evidence.

PREREQUISITES: CS3010 or CS3030, CS3600 and CS3670, or the consent of the instructor

Course Web Site

- Notes, assignments, and other stuff
  - http://www.nps.navy.mil/cs/cseagle/cs4677

Course Schedule

- Lecture
  - M-W 1400-1450, S-208
- Lab
  - Th 1300-1450, S-511

Homework/Projects

- Occasional homework assignments
  - Individual effort
  - Require some minimal internet research to supplement course material
  - Questions regarding assigned reading
- Projects
  - Teams of two, no exceptions
  - Tool familiarity
  - Forensics analysis
  - Honeynet scans of the month?

Required Text

- Jones, Bejtlich & Rose, *Real Digital Forensics,* Addison-Wesley, 2006

Other References

- Mandia, Prosise & Pepe, *Incident Response & Computer Forensics,* Osborne, McGraw-Hill, 2003
- Kruse & Heiser, *Computer Forensics, Incident Response Essentials,* Addison Wesley, 2002.
- Casey, *Digital Evidence and Computer Crime,* Academic Press, 2000.
- Sammes & Jenkinson, *Forensic Computing, A Practitioner's Guide*, Faller, 2000.

Other References (cont)

- You will also be asked to read a variety of online articles including several from:
  - http://www.honeynet.org/papers
- Consolidated list of resources
  - http://www.nps.navy.mil/cs/cseagle/cs4677/ForensicsResources.html

Rough Outline

1. Incident response background
2. Live system collection and analysis
   a. Windows
   b. Unix
3. Network evidence collection and analysis
   a. Windows
   b. Unix
4. Forensic duplication tools and techniques
5. File systems
6. Forensic analysis techniques
7. Web browser forensics
8. Email forensics
9. Windows registry forensics
10. Executable file analysis
11. Case Studies

Reading

- For Tomorrow
  - http://ftp.cerias.purdue.edu/pub/tools/unix/sysutils/tct/being-prepared.html

Forensics/Computer Forensics

- Casey:
  - The use of scientific principles or techniques that can be applied to identifying, recovering, reconstructing, or analyzing evidence during a criminal investigation
- Venema :
  - Gathering and analyzing data in a manner as free from distortion or bias as possible to reconstruct data or what has happened in the past on a system

Events of Interest - Incidents

- From *Incident Response*:
  - Unlawful, unauthorized or unacceptable action involving a computer or computer network
- Examples
  - Theft of data
  - Unlawful entry into a computer system
  - Possession of criminal content
  - Records that constitute evidence of a crime
  - Email harassment or blackmail

Incident Response

- The process of planning for, detecting, and responding to computer incidents
- Often performed by a dedicated team within an organization
  - CERT
    - Computer Emergency Response Team
  - CIRT
    - Computer Incident Response Team
  - CSIRT
    - Computer Security Incident Response Team

Incident Response Goals

- Incident verification
- Collection and analysis of evidence
- Develop case for legal action
- Protect proprietary data
- Many others

Forensics Goals

- For our purpose
  - Analysis of a computer system or systems and related data to recreate, in as detailed a manner as possible, a past sequence of events
- Class focus
  - Types of data available
  - How to collect that data
  - How to analyze that data

Forensics Response Process (SANS)

- Pre-Incident Planning
- Initial Response/Damage Control
- Evidence Recognition/Collection
- Evidence Analysis/Crime Reconstruction
- Presentation of Findings

Pre-Incident Planning

- Two types of planning
  - Organizational
    - Policies and procedures implemented prior to any incident actually occurring
  - CIRT
    - Team training
    - Construction of tool kit
      - Software
      - Hardware
      - Administrative

Organizational Planning

- Host and network based security measures
  - IDS
  - Anti-virus
  - Firewalls
  - Access controls
- Patch/Upgrade policy
- Backup policies & procedures
- End user training

CIRT Planning

- Designated incident response team
  - Beepers, cell phones, email paging capability
- Response Kit
  - Collection of hardware and software to maximize chances for successful evidence collection

Detection

- Nature of problem
- How/When/Who detected
- Hardware/software involved

Initial Response

- Determine whether an incident actually occurred
  - Could be simple software problem
  - Avoid knee jerk reactions
- Interviews
- Remote log reviews
- Minimize changes to affected system

Response Strategy

- Varies with nature of incident
  - External/internal
  - Type of attack
- Varies with importance of system
  - Critical servers
  - Firewall
  - End user system
- Extent of damage

Investigation

- Data collection
  - Most important thing is to collect in a "forensically sound" manner
    - Evidence handling
  - Host based evidence
  - Remote/Network based evidence
- Data analysis

Reporting

- Summarize incident
- Determine whether to share findings
  - Was a new software vulnerability discovered

Resolution

- Utilize findings
  - Review organizational policy
  - Repair damage
  - Upgrade systems
  - Improve security
  - Raise user awareness

CS4677 Computer Forensics Pre-Incident Planning

Chris Eagle

Fall '06

Why Plan?

- Minimize response time
- Maximize chances of successful evidence collection
- To inform people of their assigned duties ahead of time

Overview

- Assess risk
- Prepare systems for response and recovery
- Implement network security measures
- Establish policies and procedures to aid incident response
- Designate and train CIRT members
- Build CIRT response toolkit

Assess Risk

- What are you protecting?
  - Trade secrets
  - Personnel information
  - Medical information
    - HIPAA
- What is the threat?
- What is your exposure?
  - Internet? Air gapped? Wireless? Modems?

System Preparation

- Incident recognition measures
- Host based defenses
  - Personal firewalls
  - Anti-virus
  - System/Application logging
- Backup measures
  - What data? How often? Where Stored

System Fingerprinting

- One means for capturing the state of a known good system is to store a "fingerprint" of each file on the system
  - May restrict to just critical files
    - O/S and executables perhaps
  - Must store off the system to avoid compromise
- Compare files against saved fingerprints to look for changes

Hash Functions

- Generate numerical value by computing mathematical function over a data set
- A couple of definitions
  - http://en.wikipedia.org/wiki/Hash_function
  - http://en.wikipedia.org/wiki/Cryptographic_hash_function
  - http://www.x5.net/faqs/crypto/q94.html

Hash Collisions

- A given input data set will always hash to the same value
- Hash function with a small range are guaranteed to have collisions
  - Range is the number of unique values
- 32 bit results only have 2^{32} possible values
- Easy to generate collisions
  - This is a bad thing!!!

Cryptographic Checksums

- All bytes of file are run through a cryptographic hashing algorithm
  - Produces a very large value
    - This is the “fingerprint”
  - Extremely small chance of collision
  - Computationally intensive to create a file that yields a specific hash value

Common Algorithms

- MD5
- SHA-1
- SHA-256
- Others

MD5

- MD5 – Message Digest 5
  - Generates a 128 bit result (16 bytes)
  - Linux/Cygwin command:
    - `md5sum <filename>`
  - Latest cryptographic research points to MD5 being "broken"

SHA-1

- SHA1 – Secure Hashing Algorithm 1
  - Generates 160 bit result (20 bytes)
  - Linux/Cygwin command:
    - `sha1sum <filename>`
  - Perhaps also broken or soon will be

SHA-256

- SHA-256 – Secure Hashing Algorithm 256
  - Generates 256 bit result (32 bytes)
  - Not widely fielded
    - Most forensics tools do not have this built in as an automatic option yet
  - No common command line utility yet
    - Available as part of the openssl 0.9.8 tool suite
  - openssl command:
    - `openssl dgst -sha256 <filename>`

Usefulness

- Strong hash values are accepted in court as proof that two files are identical
  - Be ahead of the game and start using SHA-256
- Need to do this ahead of time
- Automated by products such as
  - Tripwire (commercial)
  - Osiris (open source)
- Must consider impact of system updates

Hash Functions in Practice

- http://www.smh.com.au/news/national/motorist-wins-case-after-maths-whizzes-break-speed-camera-code/2005/08/10/1123353388395.html
- http://www.thenewspaper.com/news/10/1033.asp
- http://townsvillebulletin.news.com.au/common/story_page/0,7034,18566295%255E421,00.html
- http://www.usdoj.gov/criminal/cybercrime/usamarch2001_4.htm

Fingerprints in Incident Response

- Compare fingerprints of existing system files with saved, known good fingerprints to isolate changed files
- What if you never did an initial snapshot?
  - OOPS!
  - www.knowngoods.org
    - Database of standard install fingerprints
  - NIST National Software Reference Library (NSRL)
    - http://www.nist.gov/srd/nistsd28.htm
    - ftp://ftp.nist.gov/pub/itl/div897/nsrl/ver_2_0/nsrl_2_0.iso

Logging/Auditing

- Unix logging
  - syslog
    - Remote logging capability
  - Process accounting
- Windows
  - *.evt files
  - Third party syslog
  - User Manager | Policies | Audit
  - File/Directory Auditing

Defenses

- Anti-virus
  - These maintain logs as well and can assist in capturing malware via quarantine features
- Keep systems patched
- Disable unused services
- Periodic checking

Network Configuration

- Firewall policies
  - What is allowed in?
  - What is allowed out?
- IDS Placement
- Maintain accurate picture of network architecture
  - Physical
  - Logical

Network Security

- Forbid protocols that pass passwords in the clear
  - SMTP, TELNET, POP3, FTP, others
- Use encrypted protocols
  - SMTP w/ TLS, HTTPS, POP3S, IMAPS, SSH, SFTP, SCP
- Authenticate users and computers

Banner Your Systems

- Login/Site bannering
  - This is a DOD computer system…. Use of this DOD computer system, authorized or unauthorized, constitutes consent to monitoring. …Use of this system constitutes consent to monitoring for all lawful purposes.
- Many legal issues surrounding monitoring
  - Consent to monitor generally gets around them
  - Improper monitoring can get you in trouble
    - Lawsuit
    - Evidence disallowed

Building A Response Team

- Outline Goals
  - Desired response time
- Select members based on desired skills
  - May be called to testify
- Training
  - Many organizations
- Practice
  - Honeynet scans of the month
  - http://www.honeynet.org

Response Toolkit

- Hardware
  - High end analysis machine
  - Large hard drives
  - Lots of RAM 1Gb or more
  - DVDRW/CDRW
  - High speed USB
  - Extra hard drives
  - Networking gear – hubs, cables
  - Tools

Response Toolkit

- Analysis Software
  - Bootable to several O/S
  - Data analysis tools
    - EnCase, FTK, SafeBack (commercial)
    - Autopsy (open source)
- Collection Software
  - Bootable CDs
    - Linux is easier here

Response Toolkit

- Collection Software
  - Trusted, statically linked binaries for evidence collection
  - Knoppix Security Tools Distribution
    - http://www.knoppix-std.org/
  - Forensic and Incident Response Environment (F.I.R.E)
    - http://biatchux.dmzs.com/

CS4677 Computer Forensics
Initial Response

Chris Eagle

Fall '06

Reading

- http://www.trouble.org/forensics/freezing.pdf
  - These are course notes so they are thin on content but full of things to think about
  - Use the rotate feature in Acrobat reader

Goals

- Rapid assessment of situation
- Appropriate escalation or de-escalation of response
- Collection of volatile evidence
- Notification of CIRT members

Initiation

- What procedures are in effect for initiating incident response
  - Should be taken care of by proper pre-incident planning
- How responsive is your front line?
  - Is it the help desk?
    - Telephone or email?
  - How about weekends?

Initial Notification

- Bomb threat style form
  - Collect as much possibly relevant information as possible
- Don't rely on email notifications or phone messages
  - These are only as good as the reporting user's technical knowledge
  - Conduct an interview

Initial Notification

- If a true incident is suspected
  - Take control of the reporting user's actions
  - Don't let them do anything to the system unless directed to do so
    - Attempt to preserve evidence
    - Attempt to contain problem

Documentation

- Document everything
  - Times, names, locations
  - Actions taken
  - Written record, voice record, photographic record

Threat Assessment

- Static situation
  - Discovery of criminal content
- Dynamic situation
  - DDoS
  - Attacker presently in a system
- Threat to organization assets

Containment

- Estimated response time
- Balance evidence collection desires against information protection requirements
  - Don't allow a hacker to play around in hopes you can observe enough activity to catch him if he is actively downloading or destroying critical data
- Assistance from outside organizations

Containment

- Consider impact of each action
  - How long can the web server be down while it is investigated?
  - Can a backup be brought online?
- Initial damage estimate
  - May influence decision to get law enforcement involved

CIRT Assembly

- Initial responders should already have been identified
  - All should be trained in proper evidence handling
  - Chain of custody starts here
- What additional skills may be required?
  - Available internally?